

**Academic Journal of Research and Scientific Publishing**

**International, peer-reviewed scientific journal**

**The 74<sup>th</sup> Issue**

**Publication date: 05-06-2025**

**ISSN: 2706-6495**

Doi: [doi.org/10.52132/Ajrsp.e.2025.74](https://doi.org/10.52132/Ajrsp.e.2025.74)

Email: [editor@ajrsp.com](mailto:editor@ajrsp.com)

### **Dedication**

It is our pleasure and great privilege to present the 74<sup>th</sup> issue of the Academic Journal of Research and Scientific Publishing to all researchers and professor who published their research in the issue, and we thank and appreciate to all contributors and supporters of the academic journal and those involved in the production of this scientific knowledge edifice.

Academic Journal of Research and Scientific Publishing

---

### *Editorial Board*

#### *Chief Editor:*

Prof. Dr. Khetam Ahmed Al-Najdi

#### *Advisory Members:*

Dr. Aicha abdelhamid eltteli abdelhamid

Prof. Dr. Riad Said Ali Al-Mutairi

#### *Editorial Members:*

Dr. Azab Alaziz Alhashemi

Prof. Dr. Khaled Ibrahim Khalil Hijazi Abu Alqumsan

Dr. Abu Obida Taha Gebreel Ali

Dr. Badreddine Berahlia,

Dr. Zainab Ridha Hammoodi Aljwaid,

Dr. Basma Mortada Mohamed Foda

Dr. Wisal Ali Al-hommada

Dr. Bilal Khalaf Ali Alzboun

Dr. Tameem Mosa Alkrad,

Dr. Walaa Al-Kurdi

Prof. Dr. Khaled Mohamed Abdel-Fattah Abu Shaira

Dr. Badir Mohamed

Dr. Abdulameer Abbas Al-khamees Ali

Dr. Nawal Hussein Siddig

Dr. Hussein Hamed Mahmoud Omer

Dr. Fatima Muflih Murshid Al-Abdlat

**Table of Content:**

No	Paper title	Author Name	Country	Field	Page No
1	A Comprehensive Review of Substrate Integrated Waveguide (SIW) Technology in the Development of 5G Microwave Components	Mansour H. Almalki, Dr. Mohammad Awedh, Dr. Mohammed N. Ajour	Saudi Arabia	Electrical and Computer Engineering	5-25
2	RSA Encryption and Decryption Implementation in an FPGA Using Verilog HDL	Dr. Mohammad H. Awedh, Dr. Ahmed Mueen	Saudi Arabia	Electrical and Computer Engineering	26-37

## **A Comprehensive review of substrate integrated waveguide (SIW) technology in the development of 5G microwave components**

**Mansour H. Almalki<sup>1\*</sup>, Dr. Mohammad Awedh<sup>1</sup>, Dr. Mohammed N. Ajour<sup>1</sup>**

<sup>1</sup>Electrical and Computer Engineering Department, Faculty of Engineering, King Abdulaziz University, P.O. Box 80204, Jeddah 21589, Saudi Arabia

\*Email: [ms.515@hotmail.com](mailto:ms.515@hotmail.com)

### **Abstract:**

This research aims to study and analyze the theoretical and technical foundations related to the design and development of microwave components used in fifth generation (5G) systems. This research focuses on Substrate Integrated Waveguide (SIW) technology, one of the most promising technologies in the field of modern communications. The importance of this research is highlighted in light of the growing need to improve the performance and efficiency of components used in wireless communication networks, especially with the development of high frequency requirements and the global transition to a fifth-generation network infrastructure.

The research addresses the problem of the limited performance of some traditional components (such as microstrip lines and rectangular waveguides) at high frequencies, in terms of signal loss, narrow bandwidth, and the difficulty of integration into printed circuit board (PCB) systems.

The research methodology relies on analyzing theoretical studies and comparing models presented in the scientific literature, without resorting to field experiments, with the aim of extracting the fundamental performance differences between conventional components and components built using SIW technology.

The research concludes with recommendations for combining SIW with modern technologies such as massive MIMO and beamforming to overcome traditional performance limitations and achieve the highest possible efficiency in future 5G networks. It also demonstrates the scientific and technical value of using SIW technology in 5G environments.

**Keywords:** 5G Microwave Components, Substrate Integrated Waveguide, Technology.

## 1. Introduction:

In recent years, the world has witnessed a tremendous boom in wireless communication technologies, particularly with the spread of fifth generation (5G) networks, which require advanced infrastructure capable of providing high speeds, low latency, and high spectral efficiency. Among the most prominent technical challenges in this field is the need to develop highly efficient microwave components, especially in high-frequency bands such as millimeter waves. Substrate Integrated Waveguide (SIW) technology is one of the most prominent innovations that has contributed to improving the performance of antennas, filters, and routers by combining the advantages of traditional hollow waves with modern manufacturing techniques on dielectric substrates.

With the rapid expansion of 5G networks, there is a need for waveguide technologies that support high frequencies and deliver high performance. Substrate-integrated waveguide (SIW) technology is a promising solution in this field, combining the advantages of traditional routers and embedded technologies, enabling the design of compact and efficient microwave components. Studies show that SIW delivers excellent performance in the millimeter-waveband, making it suitable for advanced 5G applications.

SIW technology is characterized by a decrease in signal loss compared to traditional transport lines such as microstrip, especially at high frequencies. SIW also provides easy integration with printed circuits, which reduces the size of the total system and increases its efficiency. In addition, SIW allows the design of high-quality components (High-Q) and a high energy bearing capacity, making it ideal for modern communication applications.

Despite the advantages of SIW, the design of its components faces technical challenges, such as determining the optimum dimensions of metal holes (VIAS) and the distances between them to ensure reduce signal loss and prevent radiological leakage. The transition between SIW and other transport lines requires the design of effective transformers to reduce reflections and improve compatibility. Research shows that improving these aspects can lead to a better performance of the components designed with SIW.

SIW technology is used in the design of a variety of micro -components used in 5G networks, such as filters, dividers, and couplers. Studies show that these components provide excellent performance in terms of frequency, efficiency, and small size. The use of SIW also contributes to reducing electromagnetic overlap and improving the reliability of the total system.

This analytical study aims to explore the potential of SIW technology in the design and development of microwave components for 5G networks, focusing on technical challenges and possible solutions. Through an analysis of current literature and practical experiences, the study seeks to provide useful insights for researchers and engineers in the field of microwave communications. It also hopes to shed light on future trends in the development of this technology and its applications in next-generation networks.

### **1.1. Study Problem:**

5G networks face increasing technical challenges at the infrastructure level, particularly in designing high-performance, small-sized, and low-cost microwave components. Although several conventional technologies are available (such as microstrip transmission lines and waveguides), many of them suffer from high losses, large size, or frequency limitations.

Hence, the main question of this study is:

How efficient is substrate-integrated waveguide (SIW) technology for designing and developing microwave components supporting 5G networks compared to other conventional technologies?

The following sub-questions out from the main research question:

- What are the engineering and technical characteristics of SIW technology?
- What are the basic components that can be designed using SIW (such as antennas, filters, and routers)?
- How does SIW technology compare in performance and efficiency to traditional microwave technologies?
- How compatible is SIW with 5G frequency requirements?
- What are the most notable recent studies that support the use of SIW in 5G applications?

### **1.2. Study Objectives:**

- Introduction to SIW technology and its fundamentals, and analysis of its characteristics and applications in microwaves.
- Analysis of the design of this technology's components, starting with filters, power dividers, and SIW-fed antennas.
- Determine the extent to which SIW technology contributes to improving properties such as return loss, expanding the operating bandwidth, and supporting frequencies beyond 28 GHz used in the millimeter wave bands of 5G.

- Providing a critical analytical view of the true capabilities of SIW technology and identifying the technical limitations facing its use in commercial applications.
- Providing recommendations for integrating SIW technology with modern technologies such as Massive MIMO and Beamforming.
- Clarifying the scientific, technical, and industrial value of using SIW technology in a 5G environment.
- Compiling and analyzing previous studies in this field.
- Providing recommendations for improving future designs of microwave components using SIW.

### 1.3. Study significance:

This study is of theoretical and applied importance. From a theoretical perspective, it contributes to enriching the literature on SIW technologies, while from a practical perspective, it provides an engineering reference that helps researchers and designers develop effective components for 5G networks, using technologies with small size, high efficiency, and low manufacturing costs.

### 1.4. Study Terms:

SIW – Substrate Integrated Waveguide: A technology for guiding electromagnetic waves through dielectric substrates using embedded metal holes.

5G: The fifth generation of wireless communications networks, characterized by very high data transmission speeds and operating frequencies in the millimeter wave range.

Microwave: A frequency range between 1 GHz and 300 GHz, used in communications and radar.

Resonance: A physical phenomenon in which the response of a system is amplified at a specific frequency.

### 1.5. Study structure and topics:

The study consists of the following sections and headings:

#### **Section One:** Literature Review and Previous Studies:

- Presentation of fifteen Major Studies
- Analysis and Summary of Results

#### **Section Two:** Theoretical Background and SIW Technology

- Defining SIW technology and its operating principles.



- Analyzing the design of SIW technology components.
- The efficiency of substrate-integrated wave (SIW) technology for designing and developing microwave components supporting 5G networks.
- The scientific, technical, and industrial value of using SIW technology in a 5G environment.

### **Section Three: Study Results, Conclusion and Recommendations**

#### **2. Methodology:**

This study falls within the scope of descriptive analytical research, relying on an analysis of recent scientific literature for last ten years, comparative studies, and engineering models published in reliable scientific databases such as IEEE and ScienceDirect. A number of graphs and design tables from previous studies and technical sources will also be analyzed to evaluate the efficiency of SIW compared to other technologies.

#### **3. Literature Review:**

In a study conducted by Sharma, & Singh. (2019) for Design and Analysis of Substrate Integrated Waveguide (SIW) for High Frequency Applications, high frequencies suffer from a number of factors that cause the signal to weaken or attenuate during transmission. The most prominent of these factors is atmospheric absorption, particularly due to water vapor and oxygen gas, as these gases absorb a portion of the electromagnetic energy. The researcher adopted the waveguide integrated with the substrate as an improved method for the waveguide. The SIW is a transition between a microstrip antenna and a dielectric-filled waveguide antenna. SIWs feature planar structures, allowing them to be fabricated on printed circuit boards (PCBs) and easily integrated with additional transmission lines. The design of the SIW structure was modeled and simulated on a computational machine having 2.60 GHz. 3.2 GB was the virtual memory used while computing. The study concluded that there are numerous pros for SIW over the micro-strip and DFW, SIW is low loss waveguide for the transmission of higher frequency ranges.

Vivek & Tanuj (2022) developed A circular slotted SIW guide and analytically evaluated to study its various output quality factors. After the theoretical study, various calculations of the SIW were performed with the help of MATLAB, and the design was simulated using ANSYS HFSS. The study explained the relationship between S parameters and frequency and demonstrated the range of return losses or input reflection coefficient (S11) from 10.44 GHz to 20.24 GHz and return loss drops around -51dB at 14.81 GHz. This shows that proposed SIW design is capable of beam scanning in the range of 10.44 GHz to 20.24 GHz efficiently.

A review of substrate integrated waveguide (SIW) technology, a design example and a discussion of key characteristics at 11 and 20 GHz conducted by Soundarya & Gunavathi (2020) found that SIW characteristics such as impedance is inversely proportional to dielectric constant and effective width of equivalent waveguide, whereas the phase constant is directly proportional to the dielectric constant and independent of effective width of equivalent waveguide. SIW characteristics make it a suitable candidate for miniaturized, low loss, high power handling planar components.

Nwajana et al, (2016) conducted a study titled Low Cost SIW Chebyshev Bandpass Filter with New Input/Output Connection. Using low-cost, commercially available printed circuit board (PCB) technology, A filter was designed with a center frequency  $f_0$  of 1.684 GHz; a partial bandwidth FBW of 4%; and a passband return loss RL of 20 dB. A standard low-pass filter circuit model was constructed from the standard low-pass filter. The parameters of the standard Chebyshev low-pass filter  $g$  were determined at a passband ripple of 0.04321 dB. J-inverters were used to transform the standard low-pass filter into a shunt-only network. Each shunt capacitor was designed to be equal to  $g_1$ . The simulation and measurement results show that an insertion loss of 1.3 dB was achieved across the band. The simulated and measured return losses of 15 dB and 16 dB respectively were achieved. The simulated and measured results show good agreement with the passband centered at 1.684 GHz as expected.

Hadi et al. (2020) performed a design and evaluation model of a dual-band circular aperture integrated waveguide antenna for K-band applications using an EM simulator in CST Microwave Studio. The researchers found that the SIW technology make the antenna performance enhanced in the term of matching, and this led to enhanced in the directivity and gain to make antenna suitable for K-band applications requirements.

Lalit Kumar et al. (2023). investigated and designed a spliced patch antenna (SPA) for the 5G frequencies N257 (28 GHz) and N258 (26 GHz), supported by a substrate-integrated waveguide (SIW) cavity. The researchers found that the proposed antenna has high gain, a small size, and broad spectral coverage all of which make it ideal for 5G applications.

N. Al-Fadhali et al. (2019) propose a compact, wide-bandwidth, millimeter-wave (MW) cavity-hole antenna design for 5G communications applications. The proposed antenna has an average gain of 8.574 dBi, with a compact dimension of  $20 \times 20 \text{ mm}^2$ . The antenna operates efficiently at 28 GHz and covers a wide frequency range from 22 to 30 GHz, making it suitable for various 5G applications within this band. Simulation results show that the reflection coefficients (S11) remain

below -10 dB across the entire band, indicating good radiation performance. At 28 GHz in particular, the antenna achieves high efficiency and excellent gain.

Bharti et al. (2025) designed and simulated two Gysel SIW-based power dividers operating at 15 GHz. The measured results showed isolation above 22 dB at 15 GHz, return loss better than 10 dB at each port, and an insertion loss of 2.44 dB, all of which closely match the simulated data. This demonstrates the effectiveness of the proposed design approach.

Singh and Mishra (2021) designed a compact leaky wave antenna based on a substrate-integrated waveguide (SIW) using a slot-section technique operating at millimeter-wave (mm-wave) frequency bands at 38 GHz. It was analyzed using a Finite Integration Technique (FIT)-based full-wave electromagnetic simulation tool. The radiating patch was printed on a Rogers's RT 5880 (lossy) substrate measuring  $7.5 \times 27 \times 0.254$  mm<sup>3</sup>, with a relative permittivity of 2.2 and a loss tangent of 0.0009. The antenna exhibits an impedance bandwidth of 230 MHz (38 GHz–38.23 GHz). The radiation efficiency is 82.7% with a directivity gain of 6.68 dB at 38 GHz.

Pei-Ling Chi et al. (2020) proposed a balanced filtered SIW power divider operating at two frequencies (28 and 39 GHz) for millimeter wave (5G) applications. The researchers used three SIW cavities to tune the differential and common modes and achieve dual-band pass-through with high co-pass suppression. The methodology involved designing resonant cavities, introducing isolation resistors, and achieving phase and intensity balance between the outputs. Experimental results demonstrated good performance in both bands in terms of input and output loss, isolation, and co-pass suppression (>30 dB). The study recommends the use of this design in differential air-feed networks for high-frequency systems due to its simplicity, efficiency, and small size.

Honari et al. (2017) proposed a high-gain open-loop antenna design using substrate-integrated waveguide (SIW) technology with corrugated cavities, aiming to support 5G applications in the 10 GHz band. The researchers used three layers of dielectric materials to form the antenna in a compact and lightweight manner without the need for traditional metal components. Two versions of the antenna (with two and four cavities) were tested, and the results showed that increasing the number of cavities leads to a significant gain improvement (up to 12.8 dBi), with a narrower beamwidth and improved radiation steering. The study recommends the application of this design in miniaturized 5G antennas integrated with integrated circuits.

Bhat et al. (2023) conducted a comprehensive review of substrate-integrated waveguide (SIW) technology, its pivotal role in 5G filter design, and the challenges associated with its

miniaturization. The paper highlighted the advantages of SIW technology in terms of low cost, small size, high efficiency, and easy integration with other components on printed circuit boards. It also reviewed the most prominent modern filter miniaturization techniques, such as half-mode SIW (HMSIW) and full mode SIW (FSIW) and demonstrated that these technologies enable high performance in the millimeter-wave frequency bands required for 5G networks. In terms of future direction, the study anticipated that research would focus on integrating SIW components into integrated systems-on-a-substrate (SoS) and developing low-cost, precision manufacturing processes that support mm-wave and THz applications. It also highlighted the importance of integrating this technology with CMOS and MMIC technologies to achieve higher levels of functional integration, making SIW a promising candidate for meeting the requirements of future communications networks, the Internet of Things, and smart systems.

Zhu et al. (2017) conducted a design and implementation of a broadband linear polarization antenna using substrate-integrated waveguide (SIW) technology to cover the unlicensed band from 57 to 71 GHz, a key band in 5G applications. The radiating element design is based on a complementary source combining an electric dipole and a magnetic notch surrounded by a square cavity to improve the radiation efficiency and extend the bandwidth. The core element demonstrated a bandwidth of 38.7% with an average gain of 8.7 dBi.  $2 \times 2$ ,  $4 \times 4$ , and  $8 \times 8$  arrays were formed using multi-layer SIW-based feed splitters to ensure uniform power distribution and minimize cross-polarization. The  $8 \times 8$  array achieved an experimental bandwidth of 22.9% with a maximum gain of 26.7 dBi and a radiation efficiency exceeding 80%. The results showed that using an SIW structure with integrated radiation sources provides a low-cost, high-performance, and integrable solution within future millimeter-wave communication systems, which reinforces the trend toward adopting this technology in high-capacity 5G systems.

Kumar et al. (2023) noted that maintaining a small footprint is one of the most important features of SIW antennas, as antennas with a small footprint, higher gain, and higher efficiency across a wider frequency range are more beneficial and effective. The authors designed a slotted patch antenna (SPA) for the 5G n257 (28 GHz) and n258 (26 GHz) frequency bands, supported by a substrate-integrated waveguide (SIW) cavity using RT/Duroid 5880 dielectric substrate material, with  $\epsilon_r = 2.2$  and a thickness of 0.787 mm. The antenna is excited by a  $50 \Omega$  microstrip transmission line to a transition-modulated SIW-taper to achieve optimal electrical performance. By understanding the antenna performance using the reflection coefficient (S11), radiation patterns,

and electric field distribution, the proposed antenna features high gain, small size, and broad spectral coverage, making it ideal for 5G applications.

SIW technology is complex in terms of micromanufacturing and expensive, as it requires drilling tiny metal holes. Passia & Yioultsis (2025) present a theoretical and experimental analysis of a new metamaterial-inspired planar waveguide known as the Uniplanar Single-CSRR (SIW). This structure aims to simplify the manufacturing process of high-frequency waveguides used in mmWave and 5G applications by replacing rows of metal holes with rows of grounded CSRRs, resulting in what is known as the uniplanar CSRR-SIW. Coupled mode theory (CMT) was used to accurately design and analyze the response of this structure. Results from finite element (FEM) simulations and the fabrication of an actual prototype antenna indicate that the new design offers performance comparable to conventional waveguides with simpler manufacturing and greater design flexibility, such as the ability to vary the number of CSRR rows or use heterogeneous patterns to achieve advanced functions such as dual-band or in-band blocking filters.

#### **4. Theoretical Framework:**

##### **4.1. Defining SIW technology and its operating principles**

Substrate Integrated Waveguide (SIW) technology is a recent innovation in microwave and millimeter-wave communications, representing a compromise between the advantages of traditional metal waveguides and planar transmission lines such as microstrips. The SIW structure consists of an insulating substrate covered with two metal layers on top and bottom, with two parallel rows of metal holes (vias) that mimic the side walls of a conventional waveguide. This structure enables routing characteristics similar to rectangular waveguides, with the possibility of manufacturing using printed circuit board (PCB) or low-temperature ceramic (LTCC) technologies, which reduces cost and facilitates integration with other components (Bozzi, et al; 2011).

The SIW technology operating principles:

##### **- Basic Structure:**

The SIW consists of a dielectric substrate between two metal layers (top and bottom), just like a printed circuit board.

Along the substrate, two parallel rows of metal via holes are installed. These are connected to the top and bottom metal layers, forming virtual walls that mimic the walls of a metal guide.

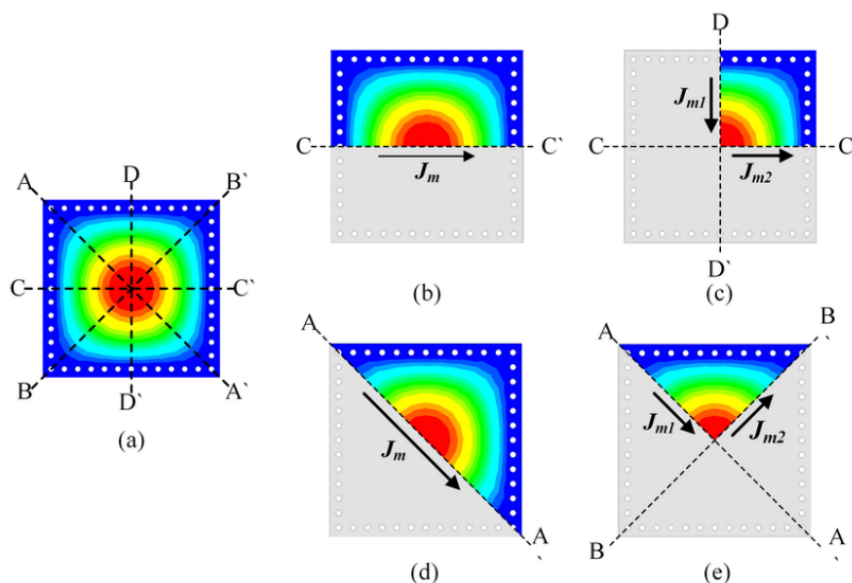
#### - Wave Transmission:

Electromagnetic waves travel within the "channel" defined by the top and bottom metal layers, with lateral boundaries formed by the two parallel rows of vias.

This structure forces the wave to propagate in a pattern similar to that of a conventional metal guide (typically a  $TE_{10}$  pattern), but on a printed, integrated substrate.

#### - Interfacing with Other Circuits:

The SIW can be easily connected to microstrips or other printed transmission lines, making it ideal for integration into microsystems or high-frequency integrated circuits.



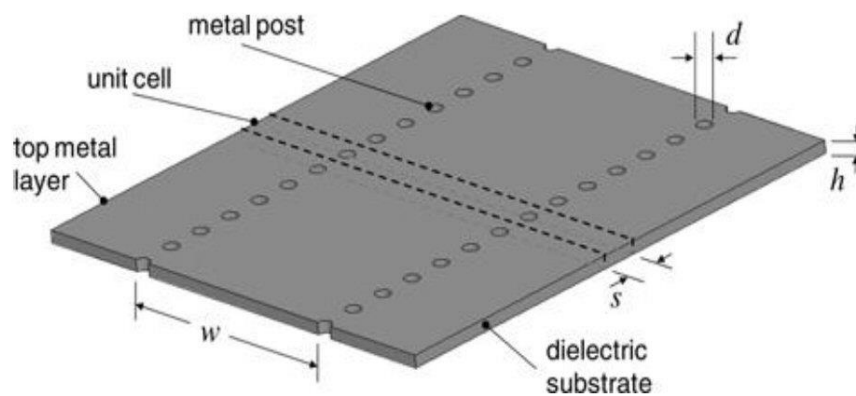
**Fig 1.** The E-field distribution diagram in the SIW cavity

The electrical distribution in this diagram in Fig.1 shows how waves travel within the SIW in a manner similar to a conventional metal guide, while maintaining the advantages of integration with printed circuits.

#### 4.2. Analyzing the design of SIW technology components

SIW is synthesized by embedding two rows of metallic vias on a dielectric substrate with top and bottom metal claddings (see Fig. 2). The 7 Via holes short both the top and bottom copper claddings so that a vertical current path exists. The propagation characteristics of SIW are almost the same as traditional waveguide.



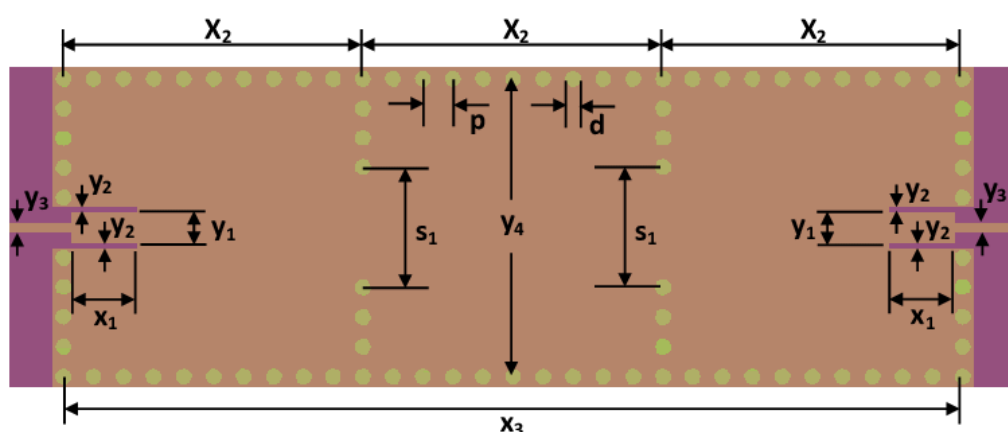


**Fig 2.** Substrate integrated waveguide (G. Soundarya and N. Gunavathi, 2020)

Where  $W$  is Substrate width,  $L$ : Substrate length,  $h$ : Substrate height,  $d$ : Via diameter,  $s$  Spacing (pitch),  $w$ : SIW width,  $w_{\text{eff}}$ : Effective width.

#### 4.2.1. Bandpass and lowpass filters:

A bandpass filter in SIW technology is a component used to pass a specific range of frequencies and block frequencies outside that range. The design is shown in Fig. 3. This type of filter is designed using resonant cavities within the Substrate Integrated Waveguide, where the pass and rejection characteristics are controlled by the dimensions and distribution of the cavities. These filters feature high efficiency and low losses, making them suitable for high-frequency communications applications such as fifth generation (5G) networks.



**Fig 3.** Substrate integrated waveguide bandpass filter layout with physical dimensions in mm ( $d = 2.0$ ,  $p = 3.725$ ,  $s_1 = 13.05$ ,  $x_1 = 8.125$ ,  $x_2 = 37.25$ ,  $x_3 = 111.75$ ,  $y_1 = 3.9$ ,  $y_2 = 0.7$ ,  $y_3 = 1.1$ ,  $y_4 = 37.25$ ). (Nwajana et al, 2016)

#### 4.2.2. S-parameters and the $S_{21}$ transfer coefficient:

Dispersion coefficients (S-parameters) are used to describe the behavior of linear electrical networks when exposed to stable electrical signals. These parameters are essential in the analysis and design of high-frequency components in substrate-integrated waveguide (SIW) technology.

Dispersion coefficients are elements of a matrix that describes the relationship between the electrical waves entering and exiting an electrical network. In a two-port network, the matrix expresses the following relationship:

In the context of substrate-integrated (SIW) routers, the  $S_{21}$  coefficient represents the ratio of the waveform coming out of port 2 to the waveform entering port 1, assuming port 2 matches the reference impedance. This is expressed mathematically as:

$$S_{21} = b_2/a_1$$

Where  $a_1$  is the wave entering Port 1 and  $b_2$  the wave coming out of Port 2. This represents the portion of the signal that was successfully transmitted through the component to the other end. The closer  $S_{21}$  is to 1 (or 0 dB), the better the signal transfer.

This parameter indicates how efficiently the signal travels through the component. In filters or routers designed using SIW,  $S_{21}$  is used to evaluate insertion loss and bandwidth.

The  $S_{21}$  factor is of great importance in SIW design, in terms of determining the efficiency of the component in transmitting the signal between ports, adjusting the dimensions of the SIW to achieve the required performance, and integration into systems by ensuring that the component is compatible with the rest of the system in terms of impedance and frequency.

The  $S_{11}$  is a measure of the amount of signal that is reflected at a specific point in the structure, usually due to a difference in the imbalance (Impedance Mismatch) or an incompatibility with the transition between the components (such as an antenna and a SIW or between two different sections of SIW). If  $S_{11} = 0 \Rightarrow$  There is no reflection (all the signal passes). And if  $S_{11} = 1 \Rightarrow$  Each sign is reflected (no energy passes). A good design goal is to have a less than -10 DB  $\Rightarrow$ , meaning that only 10% of the energy is reflected. Any repercussions that distort signal, and a loss of efficiency.

#### 4.2.3. Power dividers:

Power dividers are essential components in microwave systems, used to distribute electrical signals into multiple paths while maintaining power balance and transmission efficiency. In



substrate-integrated waveguide (SIW) technology, power dividers offer a compact and efficient alternative to conventional designs, due to their ability to reduce radiation losses and offer good compatibility with printed circuit boards. SIWs feature a compact structure and are suitable for integration with antenna systems and frequency filters in modern applications such as 5G communications and radars.

SIW power dividers are essential components in SIW antenna arrays. SIW technology replaces microstrip structures, eliminating the drawback of excessive radiation leakage at high frequencies. However, the design process for SIW power dividers is more complex than that of conventional microstrip power dividers. Farah et al. (2023) analyzed various types of T- and Y-type SIW power dividers based on their configurations, functions, and operating principles, providing guidelines including insertion loss, isolation, common phase bandwidth, return loss bandwidth, and phase balance. The researchers classified power dividers into several main types: corporate power dividers, which are further divided into single-layered and multi-layered types; series power dividers, which include HMSIW; MMIs, which include Wilkinson power dividers; Gysel power dividers; and finally, cavity-based SIWs, which include QMSIW and EMSIW.

#### **4.2.4. Power distribution range:**

The power distribution range (PDR) of substrate-integrated waveguide (SIW) technology is a key element that significantly impacts the signal transmission efficiency and power distribution in modern systems. SIW designs achieve even power distribution across multiple channels, contributing to improved overall performance of micro-components such as power dividers and antennas. This is achieved by designing SIWs that can precisely manage high frequency bands. SIWs also offer advantages such as reduced signal losses and reduced radiation losses compared to conventional designs.

#### **4.2.5. Impedance matching:**

Impedance matching is a vital factor for ensuring optimal performance in SIW systems, as it helps reduce reflection losses and improves power transfer between different components such as antennas and power dividers. When designing SIW components, it is essential that the microwave and microwave equations are matched at every point along the structure to ensure efficient signal transmission. In SIW technology, metal vias and design techniques such as narrowband expansion or slot line adjustment are used to modify the impedance and ensure that electrical components such as inputs and outputs are impedance matched.

#### **4.2.6. SIW antennas:**

SIW antennas are one of the advanced ingredients in the technology of the compact wave guide in the substrate, as it combines the advantages of traditional wave guide with integrated circuits techniques. These antennas use the compact pillars that include the rows of metal lights (VIAS) to form wave walls with characteristics similar to those in traditional microscopic waves. These antennas provide advantages such as high efficiency, simple integration with compact circles, and small size, which makes them ideal for high frequency applications such as V -5G connections (5G) and high -frequency microbial systems.

#### **4.3. Efficiency of substrate-integrated wave (SIW) technology for designing and developing microwave components supporting 5G networks.**

SIW technology is a cornerstone in the development of highly efficient microwave components that meet the requirements of 5G networks in terms of wide bandwidth, low losses, and seamless integration with miniaturized communications systems. Unlike traditional lines such as microstrips, the SIW structure offers properties similar to rectangular waveguides, enabling high signal transmission quality over frequency ranges up to tens of gigahertz, which is compatible with the mmWave bands used in 5G. Electromagnetic waves travel within a specific channel in the dielectric substrate, between two metal layers, surrounded by walls of metal holes (vias) that prevent signal leakage and maintain the wave directional pattern.

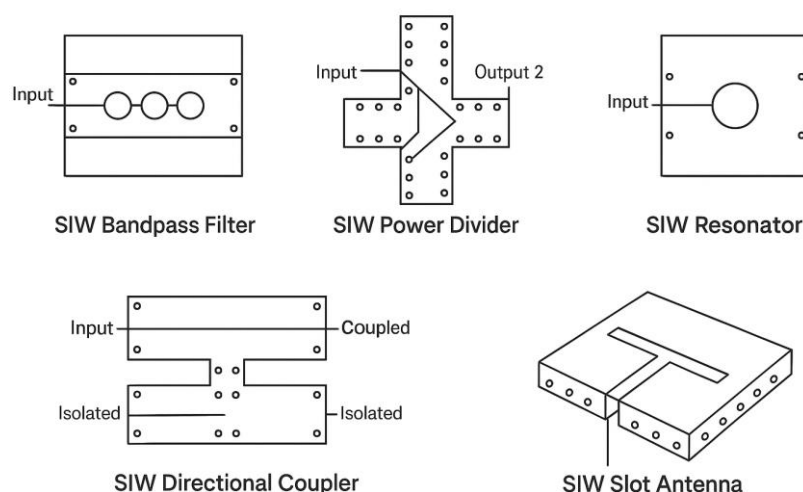
One of the most notable advantages of SIW is its high integration with printed circuit board (PCB) systems, making it ideal for designing components such as filters, power dividers, antennas, and resonators within a single environment and in miniaturized sizes. This integration reduces insertion loss and minimizes the connection problems that arise when using separate components. The SIW design also enables a relatively high Q-factor, which is essential for ensuring spectral efficiency and reducing channel interference, especially in high-spectral-density applications such as 5G networks.

Furthermore, SIW facilitates the creation of smart phased arrays at a lower cost, as they can be easily integrated with advanced feeds to support the beamforming systems used in 5G. They also offer multi-layer design capabilities, which enhances vertical space utilization and facilitates the design of integrated transceiver modules (TRx modules). With the ability to be manufactured using conventional PCB manufacturing techniques, SIWs enable low-cost, high-performance solutions, making them an ideal choice for next-generation mobile communications systems.

#### 4.3.1. 5G Microwave Components that Use Substrate Integrated Waveguide (SIW) Technology:

Substrate Integrated Waveguide (SIW) technology is widely used in the design of microwave components for 5G technologies, as it combines the efficiency of waveguide technology with PCB integration. The most important microwave components used in 5G and implemented using SIW technology include:

- Filters, which are used to separate or pass a specific frequency band, such as bandpass filters, low-pass filters, and high-pass filters. SIW makes filter designs compact, low-loss, and easy to manufacture.
- Power Dividers/Combiners: These are used to split or combine signals across multiple channels, such as the SIW Wilkinson Power Divider and the SIW T-junction Divider.
- Resonators: These are used to tune specific frequencies or to manufacture filters such as bandpass filters and sensors.
- Directional Couplers: These are used to separate a portion of the passing signal for monitoring or measurement. They provide good isolation between ports. SIW couplers provide high performance at the millimeter frequencies used in 5G.
- Antennas: SIWs integrate the antenna with the rest of the circuit, especially slot or leaky wave antennas using SIWs, SIW Slot Antennas, SIW Leaky Wave Antennas, and SIW Cavity-backed Antennas. The following Fig. 3 shows the SIW technology used in 5G Microwave Components:



**Fig 3.** Substrate Integrated Waveguide (SIW) technology That used in 5G Microwave Components. (Prepared by the Author)

The 5G components that the SIW (Substrate Integrated Waveguide) is involved in, as well as the functionality that the SIW performs within each component, can be summarized in the (Table 1). From table 1, We find that; the Substrate Integrated Waveguide (SIW) is involved in many components of the 5G Microwave and offers reduced signal loss compared to traditional lines such as microstrip, easy integration with components on the same substrate, good support for mmWave frequencies (24–100+ GHz range), and improved thermal and electromagnetic performance.

#### 4.4. The scientific, technical, and industrial value of using SIW technology in a 5G environment

##### 4.4.1. The Scientific and Technical Value of SIW Technology in the 5G Environment

Advanced Electromagnetic Integration: SIW provides an ideal environment for transmitting electromagnetic waves at high frequencies (especially mmWave) without the need for traditional metal routers, while maintaining the desired propagation patterns (such as  $TE_{10}$ ), thus enhancing signal accuracy and speed.

**Table 1. Substrate Integrated Waveguide within 5G Components and its functions.**

No	Component	SIW role within the component (function)
1	Power Dividers	Distributes the signal evenly or in a specified ratio among multiple outputs while minimizing loss.
2	Filters	Passes a specific frequency range and blocks unwanted frequencies with high accuracy and stability.
3	Waveguides	Directs the electromagnetic signal within the system with high efficiency and low loss.
4	Phase Shifters	Modifying the signal phase within the beamforming systems in antenna matrices.
5	Resonators	Generates a resonance at a specific frequency used in filters and vibrations.
6	Combiners	Merging multiple signals into one path without significant loss or unwanted overlap.
7	Directional Couplers	Isolation and division of signals to monitor them or for control and guidance uses.

8	Frequency Multipliers	Efficient generation of frequencies efficiently within the wave tracks.
9	Switches	Directing signal to different paths in the system, especially in multi -ports.
10	Amplifier Feed Lines	Modifying the signals efficiently using a low -loss path and engineering fit.
11	Integrated Antennas	Feeding the antenna with a directed signal with good radiation efficiency and reducing interference.

Efficiently Supports High Frequencies: SIW has lower losses than microstrip lines at high frequencies, making it an ideal choice for designing 5G systems based on the 24 GHz, 28 GHz, 39 GHz, and other millimeter wave bands.

Miniaturization and PCB Integration: SIW components can be implemented on printed circuit boards, allowing them to be integrated directly with other active and passive circuits, reducing the need for interconnection via cables or separate components.

Improving the performance of smart systems: SIWs effectively support beamforming and smart antenna array technologies, enhancing network coverage efficiency and reducing interference in 5G networks.

Reliability and thermal stability: Thanks to their relatively closed structure, SIWs exhibit high resistance to external interference and noise, and possess good thermal stability, which is required for 5G applications operating in harsh environments.

#### 4.4.2. Industrial value of SIW technology

Ease of manufacturing using standard PCB technologies:

SIWs enable the manufacture of high-frequency components using relatively low-cost, conventional manufacturing processes, enhancing the potential for large-scale production.

Reducing system costs:

By integrating components onto a single chip, SIWs reduce the need for external components, contributing to a lower overall system cost.

Enhancing flexibility in industrial design:

The SIW design can be easily customized to meet the requirements of diverse devices such as transceivers, 5G access points, and Internet of Things (IoT) devices.

#### 4.4.3. The Practical Industrial Applications of SIW Technology

**Bandpass/Stopband Filters:** SIWs are used to design precise filters that separate frequency channels in 5G wireless communication systems, with low insertion losses and high-specificity performance.

**Integrated Antennas:** SIWs are used to design slot antennas or integrated slot antennas on PCBs for high-frequency applications, such as transmitting and receiving stations in towers or smart cars.

**Power Dividers and Couplers:** They are used to distribute signals evenly across multiple paths within data transmission or reception units in base stations.

**High-Q Resonators:** They are used in the design of precision sensors, or as components in filters or oscillators in mmWave systems.

**Integrated Transceiver Modules (TRx Modules):** In small cells and mobile devices, SIWs are used to combine antennas, signal dividers, and frequency amplifiers into a single structure.

### 5. Conclusion:

Substrate Integrated Waveguide (SIW) technology is a superior choice for microwave component design in 5G systems, especially in high-frequency bands such as mmWave, as it offers high transmission efficiency, low loss, and good integration with printed circuit boards. Compared to technologies such as microstrip, coplanar waveguide (CPW), and traditional hollow waveguides, SIWs offer superior performance at higher frequencies, reduced unwanted radiation, and ease of integration into miniaturized systems. However, each technology has its own advantages depending on the application: microstrip and CPW are better suited for lower frequencies and lower cost, while hollow waveguides offer higher efficiency but require complex size and manufacturing. Depending on the nature of each component in a 5G system, the most suitable technology varies depending on the requirements in terms of frequency, efficiency, size, and cost.

#### 5.1. Summary of Results:

- SIW technology is used as a transmission medium in high-speed circuits, antennas, comparators, and dividers.
- SIW technology is small, inexpensive, non-dimensional, and can be easily integrated with flat transmission lines, and easy to manufacture, minimal loss and maximum power handling capacity.
- SIW technology achieves high efficiency at high frequencies (mmWave) with low radiation loss.

- SIW technology enables excellent integration with printed circuit boards (PCBs) thanks to its in-substrate construction.
- SIW technology offers performance similar to traditional hollow guides, but with a smaller size and easier manufacturing.
- SIW technology features good impedance and effective isolation between components, enhancing routing and control accuracy.
- SIW technology is ideally suited for 5G applications such as filters, antennas, dividers, and directional couplers, and it is scalable and repeatable, facilitating industrial production in large quantities.

## 5.2. Recommendations:

SIW technologies are recommended for use in advanced and complex 5G systems, particularly in base stations, radar systems, and beamforming antennas. Precise simulation tools (such as HFSS or CST) are recommended to fine-tune the design and reduce development time for SIW technology.

## 6. References:

- Khan, Z. U., Jilani, S. F., Belenguer, A., Loh, T. H., & Alomainy, A. (2018). Empty Substrate Integrated Waveguide-Fed MMW Aperture-Coupled Patch Antenna for 5G Applications. arXiv preprint arXiv:1809.07817.
- Sharma, Manvinder & Singh, Harjinder. (2019). Design and Analysis of Substrate Integrated Waveguide (SIW) for High Frequency Applications. International Journal of Innovative Technology and Exploring Engineering. 8. 944-947. 10.35940/ijitee.E3060.0981119.
- Arya, Vivek and Garg, Tanuj, Design and Analysis of Substrate Integrated Waveguide (July 14, 2022). Proceedings of the Advancement in Electronics & Communication Engineering 2022, Available at SSRN: <https://ssrn.com/abstract=4159620> or <http://dx.doi.org/10.2139/ssrn.4159620>
- Bozzi, Maurizio & Georgiadis, Apostolos & Wu, Ke. (2011). Review of substrate-integrated waveguide circuits and antennas. Microwaves, Antennas & Propagation, IET. 5. 909 - 920. 10.1049/iet-map.2010.0463.



- G. Soundarya and N. Gunavathi (2020). A review of substrate integrated waveguide (SIW) technology, a design example and a discussion of key characteristics. Dept. of Electronics & Communication Engineering, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India.
- Nwajana, Augustine & Yeo, Kenneth & Dainkeh, Amadu. (2016). Low Cost SIW Chebyshev Bandpass Filter with New Input/Output Connection. 10.1109/MMS.2016.7803795.
- Ranjesh, Nazy & Shahabadi, Mahmoud. (2008). Loss mechanisms in SIW and MSIW. Progress in Electromagnetics Research B. 4. 299-309. 10.2528/PIERB08012807.
- Hadi, Rand & Ali, Faris & Hatem, Ghufan. (2020). Dual Bands Microstrip Substrate Integrated Waveguide (SIW) Antenna for K-band Applications. Al-Furat Journal of Innovations in Electronics and Computer Engineering. 1. 1. 10.46649/300320-01.
- Lalit Kumar, Vandana Nath, BVR Reddy, (2023). A wideband substrate integrated waveguide (SIW) antenna using shorted vias for 5G communications, AEU - International Journal of Electronics and Communications, Volume 171, 154879, <https://doi.org/10.1016/j.aecue.2023.154879>.
- N. Al-Fadhali, H. A. Majid, R. Omar, M. K. A. Rahim, S. M. Shah and B. A. F. Esmail, (2019). "Wideband (22-30GHz) mm-Wave Substrate Integrated Waveguide (SIW) Antenna for 5G Applications," 2019 IEEE Conference on Antenna Measurements & Applications (CAMA), Kuta, Bali, Indonesia, pp. 1-4, doi: 10.1109/CAMA47423.2019.8959544.
- F. Bilawal, F. Babaeian, K. T. Trinh and N. C. Karmakar, (2023). "The Art of Substrate-Integrated-Waveguide Power Dividers," in IEEE Access, vol. 11, pp. 9311-9325, doi: 10.1109/ACCESS.2023.3239917.
- Bharti, B.K., Yadav, A.N. (2025). A new design technique and realization of gysel power dividers in substrate integrated waveguide for Ku-band applications. Sci Rep 15, 10844 <https://doi.org/10.1038/s41598-025-95799-w>
- U. C. Singh and R. Mishra, (2021). "Design of Substrate Integrated Waveguide (SIW) Slot Antenna for Millimeter-wave 5G Application," 2021 International Conference on Industrial Electronics Research and Applications (ICIERA), New Delhi, India, pp. 1-4, doi: 10.1109/ICIERA53202.2021.9726760.



- P. -L. Chi, Y. -M. Chen and T. Yang, (2020). "Single-Layer Dual-Band Balanced Substrate-Integrated Waveguide Filtering Power Divider for 5G Millimeter-Wave Applications," in IEEE Microwave and Wireless Components Letters, vol. 30, no. 6, pp. 585-588, doi: 10.1109/LMWC.2020.2987170.
- M. M. Honari, R. Mirzavand, J. Melzer and P. Mousavi, (2017). "A New Aperture Antenna Using Substrate Integrated Waveguide Corrugated Structures for 5G Applications," in IEEE Antennas and Wireless Propagation Letters, vol. 16, pp. 254-257, doi: 10.1109/LAWP.2016.2571280.
- Bhat, Z. A., Sheikh, J. A., Rehman, R., Khan, S. D., Bashir, I., & Ashraf, S. (2023). A survey on substrate integrated waveguide filters; design challenges and miniaturizing techniques for the 5G. International Journal of High Speed Electronics and Systems, 32(1), 2140006. <https://doi.org/10.1142/S0129156421400061>
- Zhu, Q., Ng, K. B., Chan, C. H., & Luk, K. M. (2017). Substrate-integrated-waveguide-fed array antenna covering 57–71 GHz band for 5G applications. IEEE Transactions on Antennas and Propagation. Advance online publication. <https://doi.org/10.1109/TAP.2017.2723080>
- Kumar, L., Nath, V., & Reddy, B. V. R. (2023). A wideband substrate integrated waveguide (SIW) antenna using shorted vias for 5G communications. AEU - International Journal of Electronics and Communications, 171, 154879. <https://doi.org/10.1016/j.aeue.2023.154879>
- Passia, M.-T., & Yioultsis, T. V. (2025). Analysis and experimental characterization of a uniplanar metamaterial-inspired substrate integrated waveguide for easy-to-implement mmWave components. IEEE Open Journal of Antennas and Propagation. <https://doi.org/10.1109/OJAP.2025.3556282>

Copyright © 2025 Mansour H. Almalki, Dr. Mohammad Awedh, Dr. Mohammed N. Ajour, AJRSP. This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC)

**Doi:** [doi.org/10.52132/Ajrsp.e.2025.74.1](https://doi.org/10.52132/Ajrsp.e.2025.74.1)

## **RSA Encryption and Decryption Implementation in an FPGA Using Verilog HDL**

**Dr. Mohammad H. Awedh<sup>1\*</sup>**

Associate Professor, Department of Electrical and Computer Engineering, Faculty of Engineering,  
King Abdulaziz University, Saudi Arabia<sup>1</sup>

Email: [mhawedh@kau.edu.sa](mailto:mhawedh@kau.edu.sa)

**Dr. Ahmed Mueen<sup>2</sup>**

Associate Professor, Department of Computer and Information Technology, King Abdulaziz  
University, Saudi Arabia<sup>2</sup>

Email: [mueen@kau.edu.sa](mailto:mueen@kau.edu.sa)

### **Abstract:**

The main objective of this project is to create a hardware-based system that is capable of encrypting plaintext and decrypting ciphertext when the public or private key and modulus  $n$  are given. Normally, the RSA algorithm has performance limitations in software-based realizations due to its computational difficulty in prime factorization. Our proposed design addresses this issue by utilizing the parallel processing capabilities of FPGA architectures. For efficient cryptographic processing, we have developed and optimized components such as modular multiplication and modular exponentiation using Verilog HDL. The results show that FPGA-based implementations are more suitable for secure real-time and embedded cryptographic applications as compared to traditional software approaches. Based on the result of this research the authors recommend to focus on optimizing cryptographic hardware for power efficiency and scalability, especially for use in IoT and edge devices, and encouraged to explore the integration of RSA hardware modules with other security protocols for comprehensive system-on-chip (SoC) solutions, also recommend the educational institutions and training programs to incorporate practical FPGA-based cryptographic projects to bridge the gap between theory and application and continuing to refine RSA hardware implementations and exploring new architectural strategies.

**Keywords:** Cryptography, RSA algorithm, FPGA architecture, Real-time and Embedded cryptographic, Hardware Description Language, UART.

## 1. Introduction

In modern secure communication of information systems, cryptography, the science of encoding information to protect it from unauthorized access, plays a vital role in ensuring data integrity, confidentiality, authentication, and non-repudiation. One of the most robustness and mathematical soundness cryptographic algorithms is RSA (Rivest–Shamir–Adleman) (Ugbedejo, Adebisi, Aroba, & Adebisi, 2024, pp. 1–27; Vidhyalakshmi & Ramesh, 2013). RSA algorithm is introduced in 1977, it employs asymmetric key cryptography, utilizing a pair of mathematically linked keys—one public for encryption and one private for decryption. RSA encryption offers a secure method for protecting sensitive information with its computational difficulty of factoring the product of two large prime numbers. This foundation remains an effective despite recent vulnerabilities in implementations using smaller key sizes (Zheng, 2024; Feng, Nitaj, & Pan, 2024). RSA particularly suitable for secure key exchange and digital signatures. RSA is computationally intensive, especially for large key sizes (Zheng, 2024). Traditional software implementations often face performance bottlenecks, limiting their utility in real-time or resource-constrained environments. To address these limitations, hardware-based approaches (using FPGAs) offer significant advantages. FPGAs provide performance efficiency, parallelism and re-configurability, making them ideal for accelerating cryptographic algorithms and increase their performance (Zhang & Zhang, 2012).

In this paper, we present the design and implementation of an RSA encryption/decryption system on an FPGA using Verilog HDL. The primary objective is to develop a high-performance, hardware-optimized cryptographic engine capable of securely processing data in real-time. By focusing on the implementation of modular multiplication and modular exponentiation, the core operations in RSA, our work demonstrates the effectiveness of FPGA platforms in handling the computational demands of public-key cryptography.

## 2. Related Work

Significant research efforts have been made on the RSA encryption algorithm using Verilog HDL on FPGA platforms for hardware implementation. Addressing different aspects of the research, such as performance optimization, architectural innovation, and design challenges. An encryption engine was generated in study of Vidhyalakshmi and Ramesh (2013), focusing on key creation, encryption, and decryption processes. The method the researchers used is right-to-left binary exponentiation and utilizes a primality tester for random prime number generation.

They used Verilog coding for the implementation and synthesized using the Xilinx 13.2 design suite. The results show that it is an efficient approach to RSA encryption at moderate key sizes. The design and verification of an RSA encryption system were identified in study of Zhang and Zhang (2012). The main goal of the research was to improve modular operation efficiency. The study emphasized improving modular operation efficiency through Montgomery modular multiplication.. The method and design researchers introduced have successfully decreased computational complexity. It makes the system very suitable for real-time cryptographic applications on FPGA platforms.

The work by Alshahrani (2017) also focused on implementing RSA using Verilog HDL. The complete details have been given for key generation, encryption, and decryption. The study also provided valuable details about the challenges often experienced during hardware implementation phases.

In study of Arun and Dharani (2020), the Shift-Sub Modular Multiplication (SSMM) algorithm was introduced. The research presents a division-free approach to modular multiplication. The RSA cryptosystem was implemented using Verilog HDL. The result of the performance comparison shows efficient gains in specific operational contexts by traditional Montgomery multiplication techniques. A different mathematical approach was presented in study of Raut and Raut (2006). The method from Ancient Indian Vedic Mathematics was employed to design the RSA cryptosystem. This research work utilized a hierarchical overlay multiplier architecture and a Straight Division algorithm. The system decreases hardware complexity and increases performance when synthesized on Xilinx Spartan FPGAs. Using larger key sizes by expanding the RSA implementation is proposed (Abid & Khan, 2019). The design is an RSA encryption incorporating Montgomery modular multiplication using Verilog HDL, which improved efficiency. The research provided a comprehensive hardware implementation and simulation. The proposed approach shows the effectiveness when security is important.

A comparative study was conducted by Kochte et al. (2016), which analyzed different FPGA-based architectures for RSA implementation. The study examines different features of concurrency and sequential operation designs. This research work discussed in detail resource utilization and power consumption. Research assists designers in selecting appropriate architectures based on system requirements.

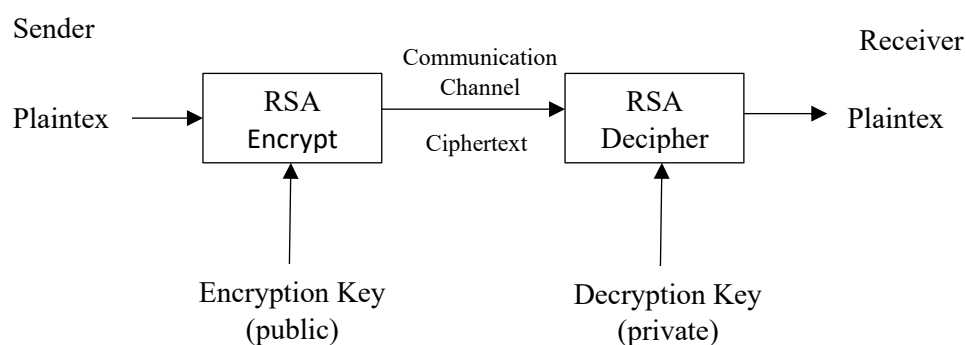
Saini (2017) presented an efficient primality testing algorithm optimized for 64-bit RSA encryption. They have used the right-to-left binary exponentiation method. The approach is suitable for constrained hardware environments by providing enhanced performance while minimizing FPGA area usage. The study by Kumar and Sharma (2015) utilized Montgomery multiplication with Block RAM (BRAM) blocks to store operands. The design achieved a suitable and efficient RSA operation by avoiding hard-wired modulus values and dynamically managing operands.

The above-mentioned research work collectively explains the different techniques and designs. Studies investigated hardware implementation of RSA encryption by highlighting improvements in speed, resource utilization, scalability, and overall system efficiency.

### 3. RSA Cryptographic Communication Model

The RSA Cryptographic Communication Model is a framework that explains how the RSA cryptographic algorithm is used to ensure secure communication between two parties over an insecure channel.

Figure 1 illustrates the fundamental working of the RSA public-key cryptographic algorithm. The process starts when the sender wants to send a confidential message. This message is in readable form, which is referred to as a “plaintext”. To ensure secure transmission, the plaintext is encrypted using the receiver’s public key via the RSA encryption module. The output of this process is ciphertext. The communication channel is used to transmit the ciphertext. This channel is supposed to be insecure, but due to the features of RSA encryption, the message remains secure. The ciphertext cannot be decrypted without a private key. To receive the ciphertext, the receiver uses the RSA decipher module to convert the ciphertext back into readable plaintext. The private key, which is kept confidential, is used during the decryption process in which it is applied to decrypt and recover the message.



**Figure 1:** RSA process model

### 3.1. General steps of RSA

The RSA process involves three key steps: (Educative.io, 2025)

1. Key Generation: In this step, the public,  $(e, n)$ , and private key,  $(d, n)$ , are created. Two large prime numbers,  $p$  and  $q$  are generated. Then, we compute  $n = p \times q$  where  $n$  is used as the modulus for both the public and private keys. Then, we calculate Euler's totient function:

$$\phi(n) = (p - 1)(q - 1).$$

Next, we choose a public exponent  $e$ , where  $1 < e < \phi(n)$  and  $e$  must be co-prime to  $\phi(n)$  (i.e.,  $\gcd(e, \phi(n)) = 1$ ). Then, we compute the private exponent  $d \equiv e^{-1} \bmod \phi(n)$ . In other words,  $d$  is the modular multiplicative inverse of  $e$  modulo  $\phi(n)$ .

2. Encryption: Given a plaintext message  $M$  (as an integer), using the public key  $(e, n)$ , we compute the ciphertext  $C$  as:

$$C = M^e \bmod n$$

3. Decryption: To recover the original message  $M$  from the ciphertext  $C$ , we use the private key  $(d, n)$ :

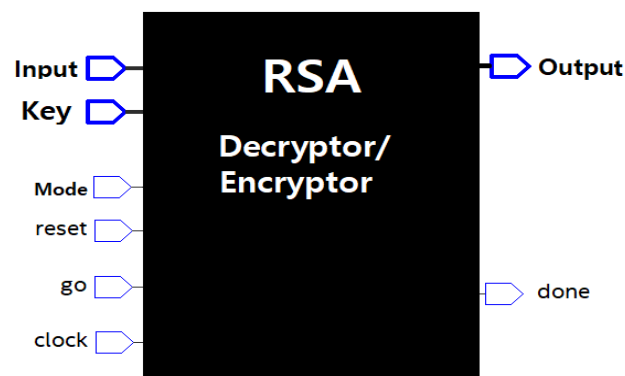
$$M = C^d \bmod n$$

Since RSA is considered an Asymmetric key procedure, its security relies partially on the fact that it's easy to choose two random prime numbers, but it's very hard to discover what they are when just given the product of them.

Therefore, typical key sizes are 1,024 or 2,048, or 4,096 bits, unlike Symmetric keys, which are much smaller. The reason RSA is large is that's because there are only so many prime numbers of that size and below. The RSA scheme can only use pairs of prime numbers, whereas the symmetric schemes can use any number of the same size (Educative.io, 2025). But for the sake of simplicity and practicality, we used a small key length in the code.

### 3.2. Black Box Design

To implement a secure RSA cryptographic system in hardware, both the encryption and decryption algorithms need to be translated into a form that can be executed on digital circuits. This is achieved using Verilog HDL (Hardware Description Language). Figure 2 illustrates the basic I/O of our design, which utilizes the two control signals “go & done” and a reset signal to abort operations, and of course, a clock.



**Figure 2:** General Black Box Design

The main I/O here are the mode, key, Input, and Output.

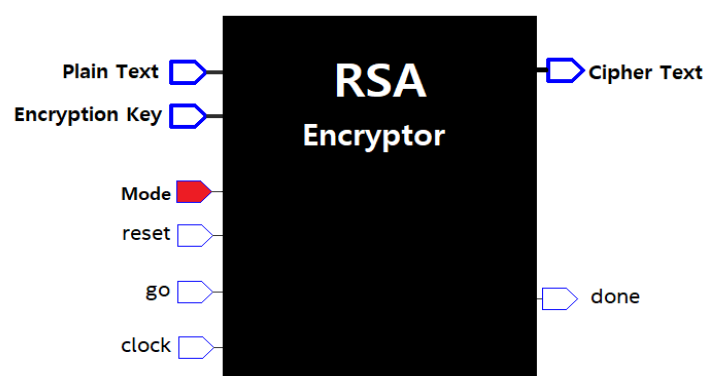
**Mode:** will control which state the digital circuit should be in, either Encryption state or Decryption state.

**Key:** is the key pair, it depends on whether the Encryption/Decryption mode is chosen.

**Input:** is going to be either Plaintext or ciphertext, depending on whether Encryption / Decryption mode is chosen.

**Output:** is going to be either Ciphertext or Plaintext, it depends on whether Encryption / Decryption mode is chosen.

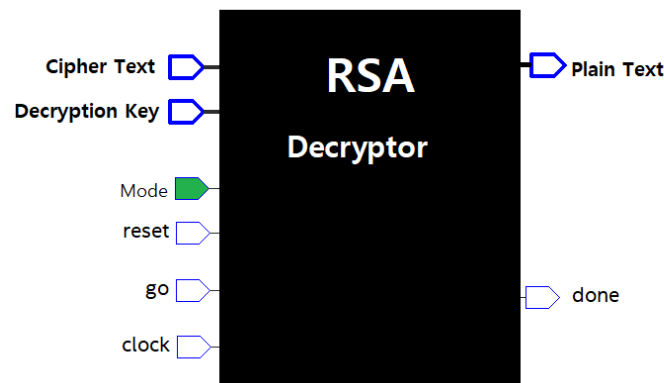
In Figure 3 RSA encryptor takes the encryption key, a mode selection, reset, a 'go' signal to initiate encryption, and a clock signal for synchronization as inputs for plaintext. The encryptor produces ciphertext as its main output and a 'done' signal to indicate completion of the encryption process.



**Figure 3:** Black Box Design in Encryption state



Figure 4 depicts the RSA decryptor module, which accepts an encrypted message as input (Ciphertext), private key (Decryption Key), control signals (Mode, reset, go, clock) as inputs. The decryptor produces an unencrypted message (Plaintext) as output and indicates done as completion.



**Figure 4:** Black Box Design in Decryption state

### 3.3. Control Unit Implementation using One-Address ROM

Table 1 presents our control unit implemented using a One-Address Read-Only Memory (ROM). The table explains the control logic based on the current state and the input test conditions by identifying the next state and the control signals.

STATE	AB	TEST	NST	Load	Runinng	Done
$S_0$	00	00	00	0	0	0
$S_1$	01	10	10	1	0	0
$S_2$	10	01	10	0	1	0
$S_3$	11	11	00	0	0	1

**Table 1:** Control Unit One Address ROM table

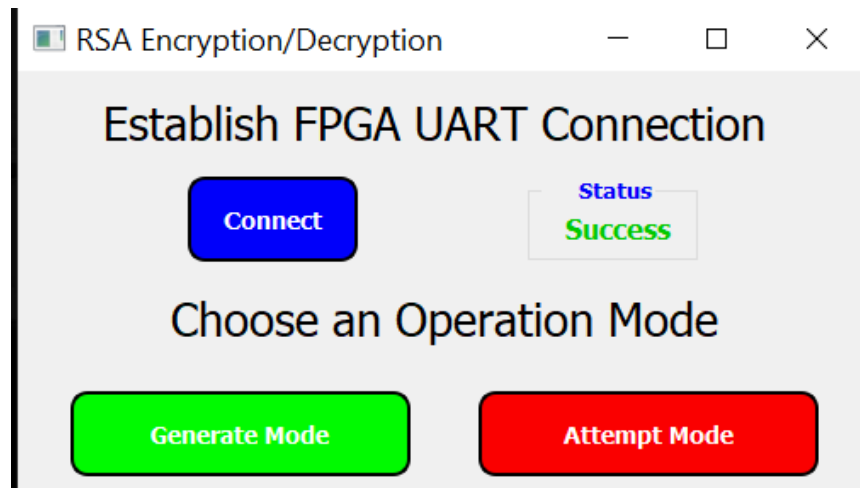
In the control unit, the current state “AB” and the input test condition “TEST” both produce the address to the ROM. The contents of the ROM store the next state “NST” and all the values for the control signals Load, Running, and Done. For example, if the current state  $S_1$  is ‘01’ and the test input is ‘10’, then the ROM is addressed with ‘0110’. The next state  $S_2$  would be ‘10’ followed by the control signal values ‘1’, ‘0’, and ‘0’.

### 3.4. RSA Encryption Decryption System

The RSA encryption and decryption system is an important component of secure digital interactions due to its mathematical foundation and good track record. In our system, we first establish Universal Asynchronous Receiver-Transmitter (UART) communication with the FPGA

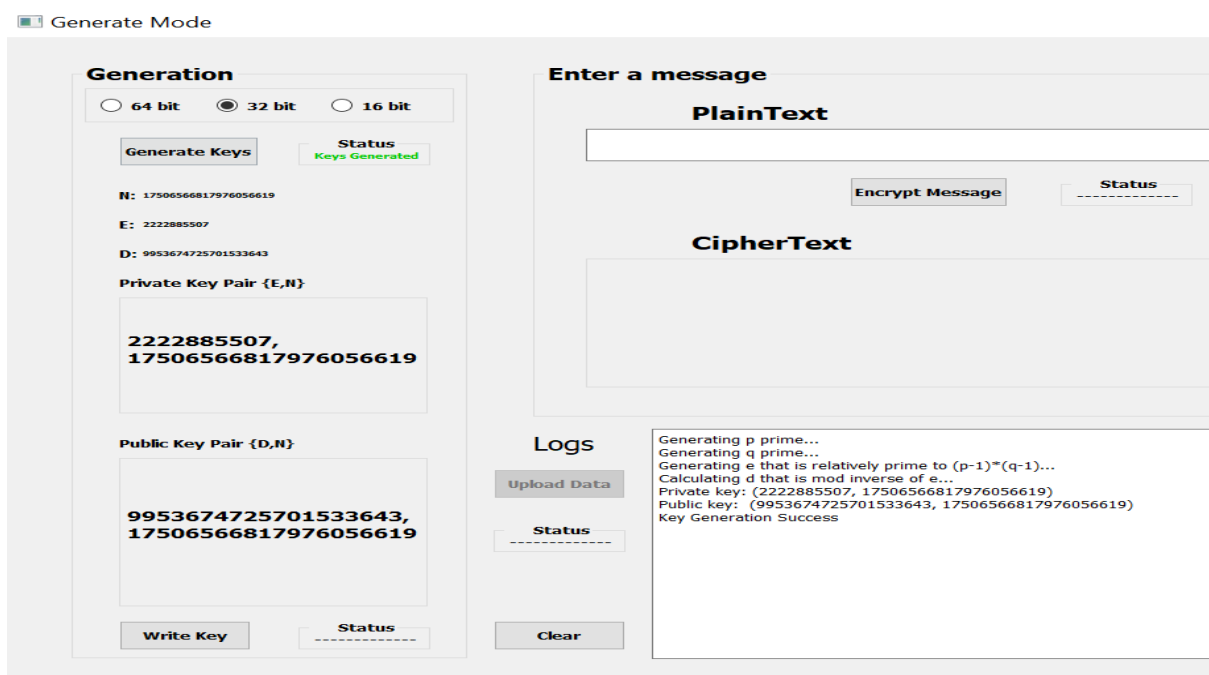


for the implementation of the RSA algorithm, as shown in Figure 5. The UART provides a serial communication protocol that helps us to send commands to the FPGA and receive the results of the RSA operations.



**Figure 5:** UART communications with the RSA FPGA

After establishing the UART communications, the mode buttons get activated. The “Generate Mode” is where the keys are generated and the plaintext is encrypted with the private key, and the public key is printed onto an RFID key. We choose the prime numbers bit size from the radio buttons in the generate mode window and click the “Generate keys” button to create the key pairs needed, as shown in Figure 6.



**Figure 6:** Generate window

We can enter our desired plaintext and press “Encrypt,” which will transfer its integer value over to the FPGA to be encrypted. Then we can press the “Upload Data” Button to post our ciphertext on the cloud as in Figure 7.



Figure 7: Encrypt message window

In the attempt mode, the user can go over to another computer and do the same steps for establishing UART communication with the FPGA. Pressing “Fetch” in the attempt window will fetch the ciphertext from the cloud and display it as shown in Figure 8.

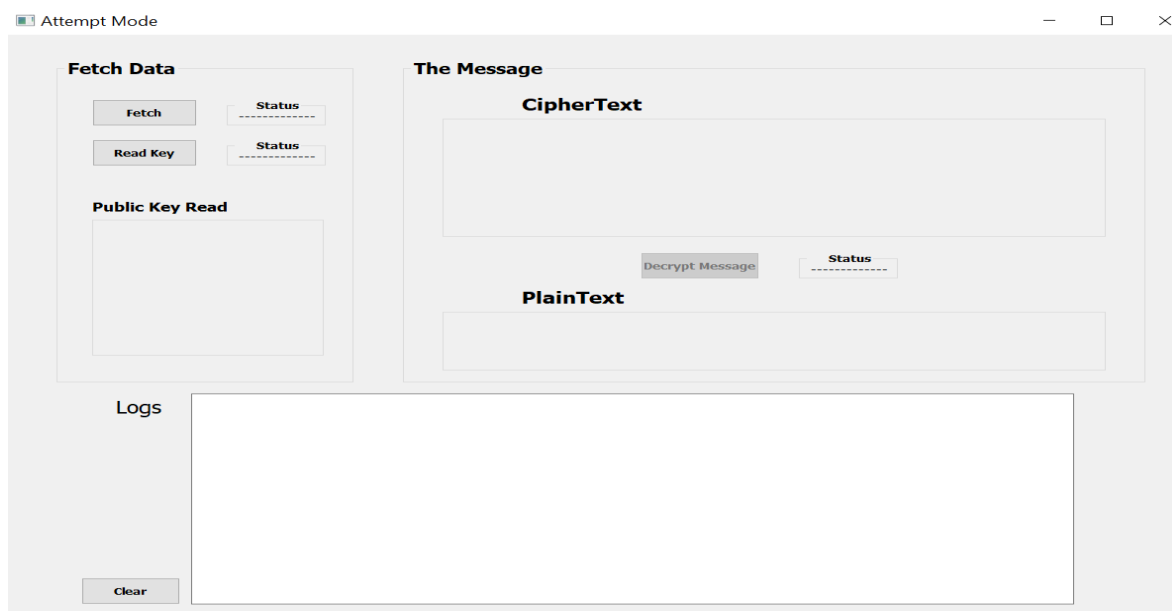


Figure 8: Attempt window

Then pressing the “Read Key” button when placing an RFID Tag over the Reader decodes the public key on it, as shown in Figure 9.

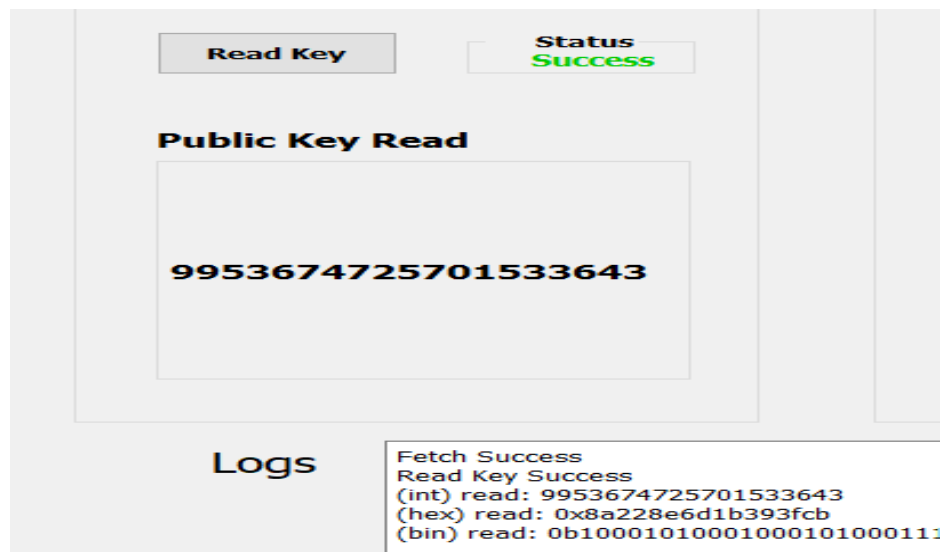


Figure 9: Public key read

Finally, in Figure 10, with the public key at hand and the ciphertext, we can decrypt our message by sending the data over to the FPGA and receiving back the integer, which will be converted to a readable string plaintext.

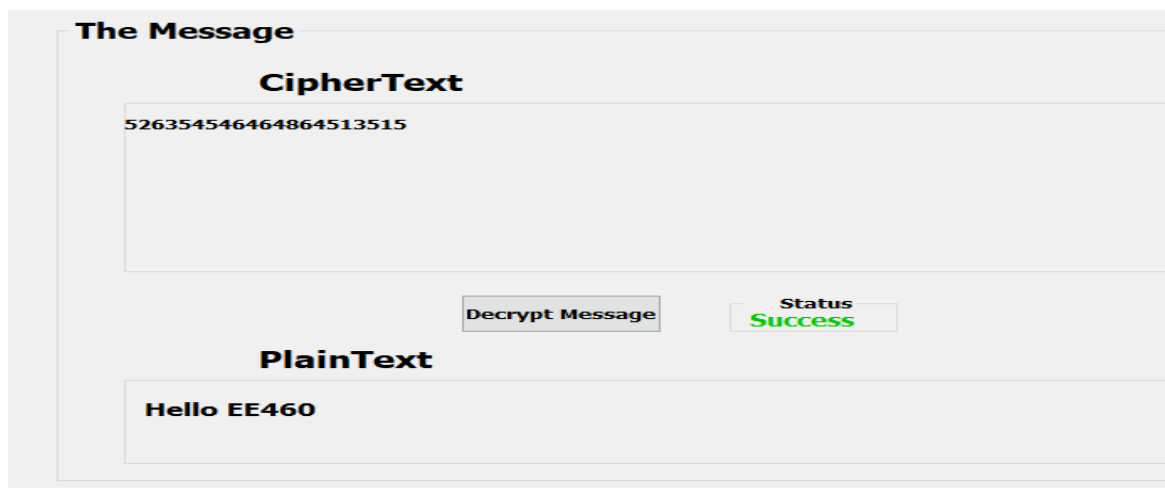


Figure 10: Decrypt message

#### 4. Conclusion and Recommendations:

In this work, we have implemented the RSA algorithm on an FPGA using Verilog HDL. Our research focus was to develop a hardware-based system that can efficiently handle the computational requirements of RSA, mainly modular multiplication and exponentiation. The result shows that FPGA-based implementations have an advantage over software-based approaches for real-time and embedded cryptographic applications.

## Recommendations:

- The research community must focus on optimizing cryptographic hardware for power efficiency and scalability, especially for use in IoT and edge devices.
- Researchers are encouraged to explore the integration of RSA hardware modules with other security protocols for comprehensive system-on-chip (SoC) solutions.
- Future research can investigate implementing RSA with larger key sizes or combining it with other cryptographic algorithms such as AES to enhance performance and security in hybrid systems.
- In digital system design, educational institutions and training programs should incorporate practical FPGA-based cryptographic projects to bridge the gap between theory and application.

The research community can contribute to more efficient, secure, and practical cryptographic systems by continuing to refine RSA hardware implementations and exploring new architectural strategies.

## 5. References

- Abid, H., & Khan, M. F. (2019). 1024-bit RSA encryption algorithm design using Verilog and FPGA implementation. *International Journal of Engineering and Advanced Technology (IJEAT)*, 8(5).
- Alshahrani, A. (2017). *Implementation of RSA in Verilog*. California State University, ScholarWorks Projects.
- Arun, T. P., & Dharani, V. (2020). Verilog HDL implementation for an RSA cryptography using shift-sub modular multiplication. *Journal of Intelligent and Fuzzy Systems*, 17(3).
- Educative.io. (2025). What is the RSA algorithm. Retrieved April 10, 2025, from <https://www.educative.io/answers/what-is-the-rsa-algorithm>
- Feng, Y., Nitaj, A., & Pan, Y. (2024). Partial prime factor exposure attacks on some RSA variants. *Theoretical Computer Science*, 999, 114549.
- Kochte, M. A., et al. (2016). Comparison of high concurrency and sequential architectures for RSA on FPGAs. In *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE)*.
- Kumar, M., & Sharma, S. (2015). Efficient RSA implementation using block RAMs and Montgomery multiplication. *International Journal of Computer Applications*, 111(4).

- Raut, R., & Raut, S. (2006). VLSI implementation of RSA encryption system using ancient Indian Vedic mathematics. arXiv preprint arXiv:cs/0609028.
- Saini, C. S. (2017). Design and FPGA implementation of 64-bit RSA cryptosystem. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 5(4).
- Ugbedeoj, M., Adebiyi, M. O., Aroba, O. J., & Adebiyi, A. A. (2024). RSA and elliptic curve encryption system: A systematic literature review. International Journal of Information Security and Privacy, 18, 1–27.
- Vidhyalakshmi, S., & Ramesh, N. (2013). Cryptosystem: An implementation of RSA using Verilog. International Journal of Computer Applications, 64(17).
- Zhang, L., & Zhang, H. (2012). RSA encryption algorithm design and verification based on Verilog HDL. In Proceedings of the 2nd International Conference on Computer Science and Electronic Technology.
- Zheng, M. (2024). Revisiting small private key attacks on common prime RSA. IEEE Access, 12, 5203–5211.

Copyright © 2025 Dr. Mohammad H. Awedh, Dr. Ahmed Mueen, AJRSP.

This is an Open-Access Article Distributed under the Terms of the Creative Commons Attribution License (CC BY NC)

**Doi:** [doi.org/10.52132/Ajrsp.e.2025.74.2](https://doi.org/10.52132/Ajrsp.e.2025.74.2)